

# 區域網設備發現之Bonjour協議

2016-09-28 由 嵌入式企鵝圈 發表于科技

在WIFI物聯網解決方案中，通常我們需要對設備進行綁定，需要通過某種方法先對設備進行發現，比如微信硬體採用廣播的方式，定時向外發送上線消息或者採用一問一答的方式進行發現，Bonjour是由蘋果公司實現的一種零配置網絡(Zeroconf)協議，它是一種基於服務的設備發現協議，不僅能夠自動獲取有效IP位址，還可以通過查詢服務的方式來找到設備地址，只要雙方約定好服務(service)的名稱，設備的IP位址和埠都是可以變化的！

## 一、mDNS協議和DNS-SD協議

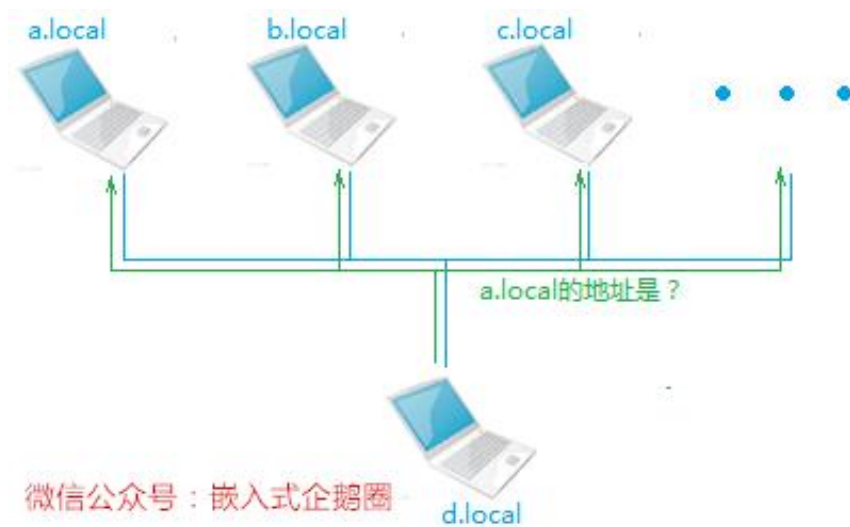
Bonjour協議是基於mDNS(Multicast DNS)協議和DNS-SD(DNS Service Discovery)協議開發實現，因此有必要先在這裡給大家介紹一下這兩個協議。

### 1.1 mDNS協議介紹

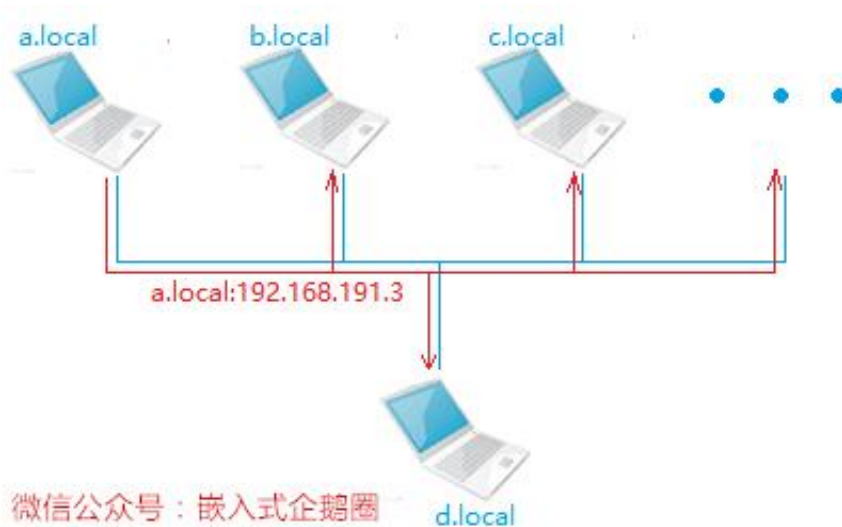
mDNS協議適用於區域網內沒有DNS伺服器時的域名解析，設備通過組播的方式交互DNS記錄來完成域名解析，約定的組播地址是：224.0.0.251，埠號是5353，mdns協議使用DNS協議一樣的數據包，由頭部和數據段兩部分（大家可以自行去了解DNS數據包的格式啦，在這裡不展開介紹了）：

offset (bytes)	0	1
0	ID = 0x0000	
2	Flags	
4	QDCOUNT	
6	ANCOUNT	
8	NSCOUNT	
10	ARCOUNT	
12	Data 微信公众号：嵌入式企鵝圈	

mDNS的一個使用情景是這樣的：



設備d通過組播（224.0.0.251：5353），詢問a.local地址是？



設備a知道有人查詢它後，也是通過同樣的組播組回復它的地址信息（通過回復用於IPv4的A類型DNS記錄(A Record)或者用於IPv6的AAA類型的DNS記錄，A記錄和AAA記錄分別用於將域名轉換成IP位址），這裡組播內的所有人b, c, d都會收到，它們會將a.local的ip地址等信息（如TTL值）刷新到mDNS緩衝區中。

mDNS協議和DNS協議還有些不同，mDNS只能用於區域網內部，並且它只接受解析主機名前綴為.local的域名，因此mDNS也是可以和DNS在同一台設備上共存的，以及它們存儲記錄的區域是分開的。

除此之外，mDNS還有其它的作用，例如在零配置網絡中給自己分配域名，設備給自身選擇一個域名後，然後通過發送記錄類型為「any」的mDNS包來查詢區域網內是否有同名，如果沒有設備就會把這個名字作為自己的域名。

## 1.2 DNS-SD協議介紹

接下來再介紹一下DNS-SD協議，即DNS based Service Discovery，基於DNS的服務發現主要用到DNS現有的三種類型記錄(Record Type)：PTR記錄、SRV記錄、TXT記錄，其中：

1) 服務發現：設備會先發送一個查詢PTR記錄的數據包到組播組，所查詢服務格式為：

`<service>.<transport>.<domain>`

**service**表示的是要查詢的服務，**transport**表示的是傳輸的協議：TCP還是UDP，**domain**表示查詢的域，在mDNS中為.local，接著具有對應服務的設備會響應一系列本設備上所具有的服務實例：

`<instance>.<service>.<transport>.<domain>`

**instance**表示服務的實例名，雖然收到`<instance>.<service>.<transport>.<domain>`，但是只有**instance**才會顯示給用戶看，比如：要查詢一個`_easylink._tcp.local`的服務，具有這個服務對應實例的設備會響應一條PTR記錄：`EMW3031 Module#500A3F._easylink._tcp.local`，即表示EMW3031 Module#500A3F為`_easylink._tcp.local`的一個實例，設備收到後只會顯示`EMW3031 Module#500A3F`供用戶看，它是UTF-8編碼的。

可以看出，DNS-SD的PTR記錄所代表的意思是區別於傳統DNS的PTR記錄的含義的，並且DNS-SD下的PTR記錄用於記錄服務到服務實例的映射。

2) 獲取服務實例的主機名和埠號：上述多個服務實例**instance**顯示供用戶選擇確定一個後，就需要查詢記錄服務實例的主機名和埠號，即查詢SRV記錄。

設備會發送一個mDNS請求，然後具有所請求中服務實例的設備會響應SRV記錄，SRV記錄記錄了這個服務實例對應的主機名和埠號以及TTL信息，一條SRV記錄的例子是：

`EMW3031 Module#500A3F._easylink._tcp.local. 3 IN SRV 0 0 8002 EMW3031 Module#500A3F.local.`

DNS下的SRV記錄的格式為：

`_service._proto.name. TTL class SRV priority weight port target.`

在DNS-SD中，**priority**和**weight**無效，一般置為00 00，**port**和**target**即為埠號和主機名。

因此**SRV**記錄用於記錄服務實例到埠號和主機名的映射，即便埠號可變也沒有關係。

3) 服務實例更詳細的信息：有時候，一個服務實例除了所在設備的埠號和主機名這些信息以外，還可以提供更多的附加參數信息，服務實例的附加信息記錄在**TXT**記錄中，以「**key = value**」的格式記錄，如提供設備的**MAC**地址：

**MAC=D0:BA:E4:50:0A:3F**

## 二、Bonjour協議原理

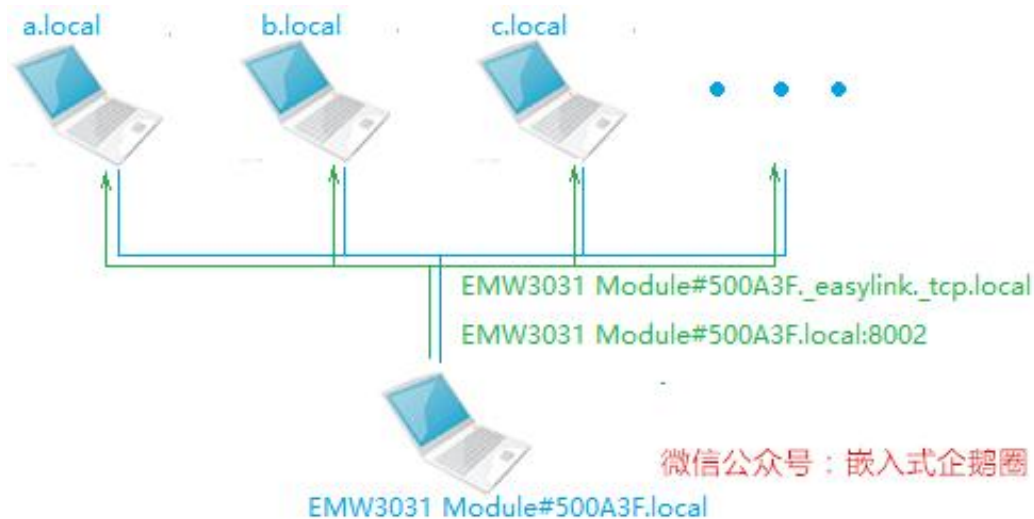
前面介紹了**mDNS**協議以及**DNS-SD**協議，其實基本上就已經展開介紹了**Bonjour**協議的細節，接下來再來理解**Bonjour**就相當輕鬆了。**Bonjour**協議可以理解為**mDNS**協議和**DNS-SD**協議的結合，其實大家在繼續往下看之前可以自己想一下如何將兩個協議結合起來呢？**DNS-SD**已經找到了提供服務的埠號和主機好了，最後再做進一步的主機名到**IP**位址的解析就完成了**Bonjour**協議的整個過程，當然結合的時候**DNS-SD**所發送的三種記錄都是通過**mDNS**規定的組播組和埠號（**224.0.0.254**：**5353**）發送出去的，但是**DNS-SD**是不依賴**mDNS**協議而存在的。

**Bonjour**協議提供三部分功能：通告服務、發現服務、解析服務，這是三個動賓詞組哈。在物聯網中，設備在本地記錄一個服務往往需要提供服務相關的**SRV**記錄、**PTR**記錄以及**TXT**記錄相關的信息，用於最後組裝**mDNS**數據包發送出去。

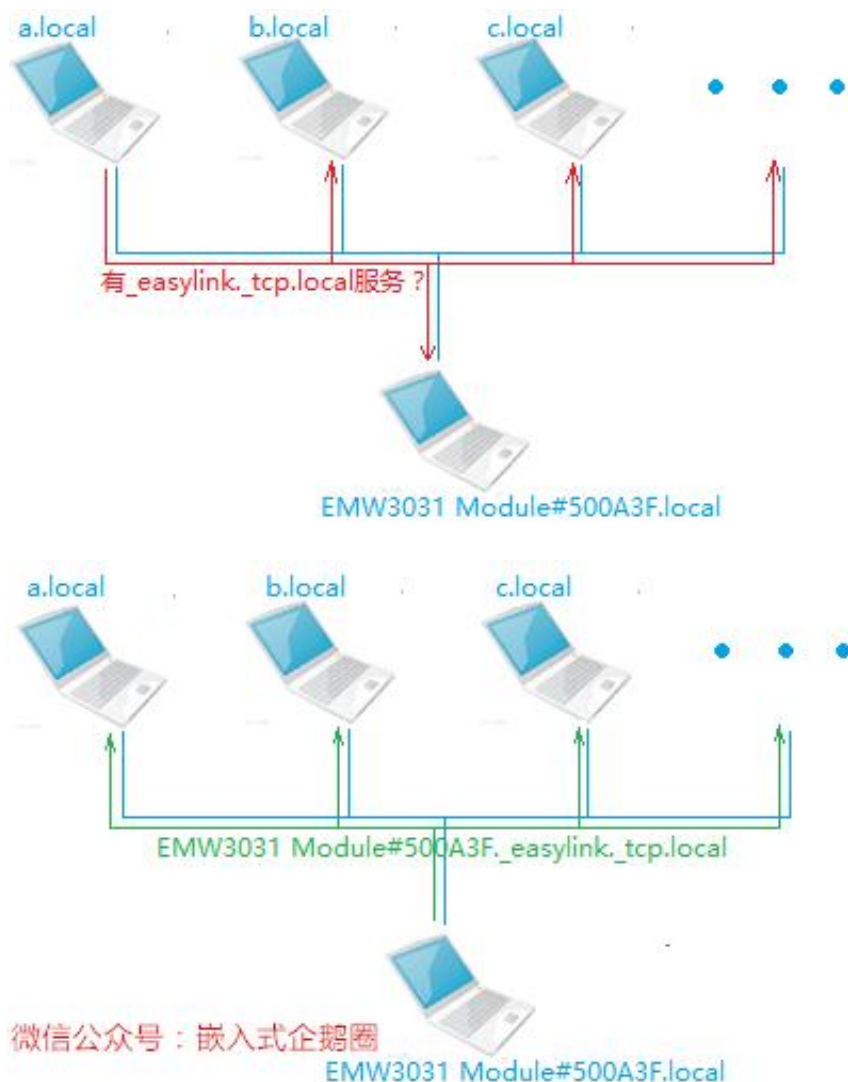
在沒有**DHCP**分配**IP**位址和沒有設置靜態**IP**位址情況下，通過**Bonjour**協議還可以在區域網內獲取有效的**IP**位址以及主機名，但是需要我們配置好路由的信息如子網掩碼等，它會生成一個**IP**，然後詢問區域網內是否有衝突，如果沒有衝突就將這個**IP**占為己有，如果有衝突，就會更換一個**IP**，繼續查詢，主機名也是利用同樣的方法獲得。

通告服務用於設備告之區域網內其他人本設備的服務信息，一般包括發送**SRV**記錄

和PTR記錄，這些記錄被其它mDNS設備記錄在本地的存儲區中。

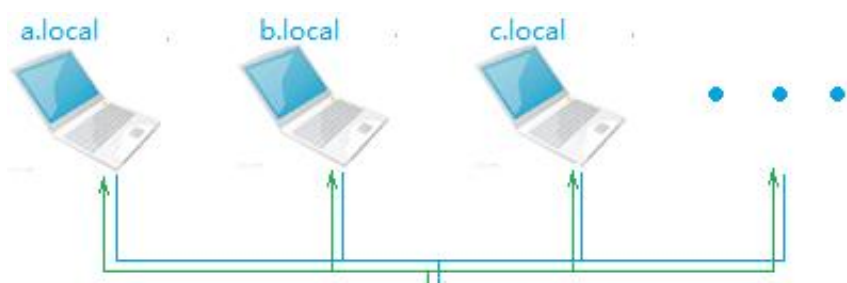
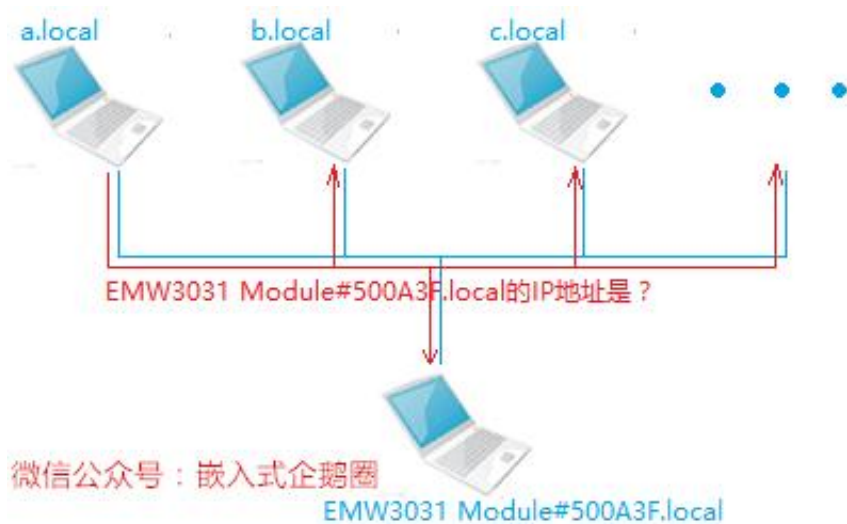
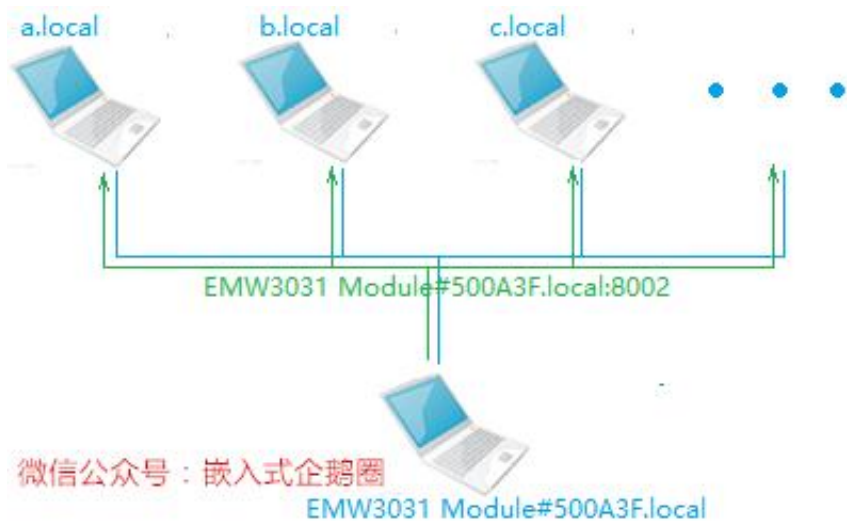


發現服務用於查詢一個指定的服務，然後具有該服務的設備會響應PTR記錄，告訴查詢的設備有這樣的服務並且服務實例的名稱是什麼。



解析服務發生在完成服務發現之後，獲得了服務實例後供用戶選擇，再下一步就要進行解析，首先根據服務實例獲得該設備的主機名以及埠，最後再根據主機名來獲

取IP位址。





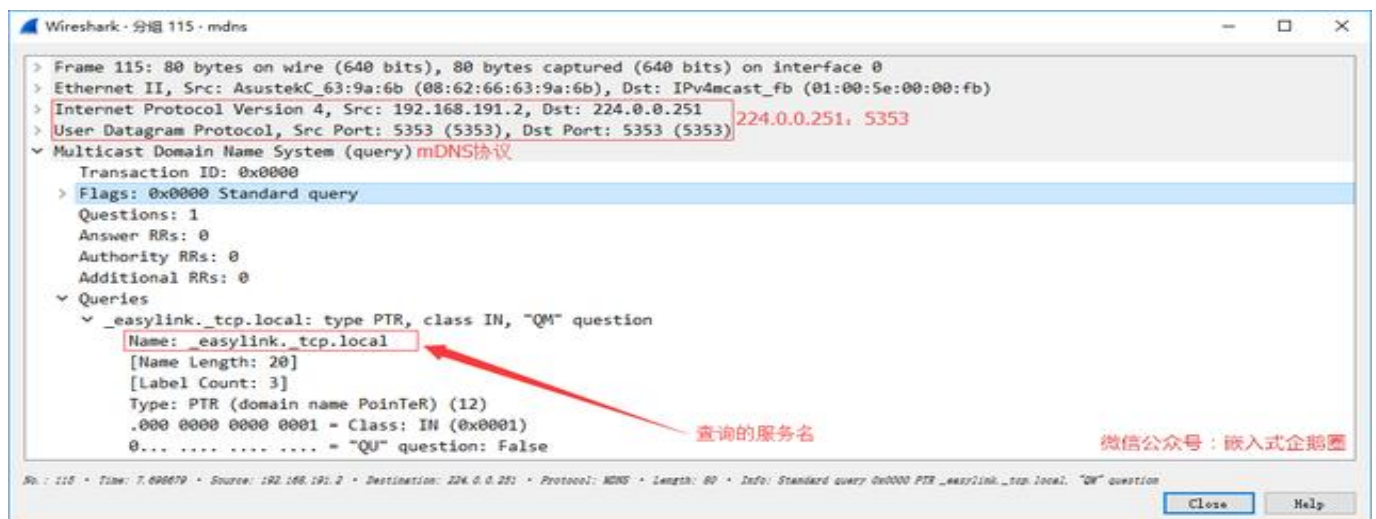


經過以上一步步交互就可以獲得了目標設備的IP位址和埠號了，然後就可以根據選擇的傳輸協議TCP或者UDP進行通信。

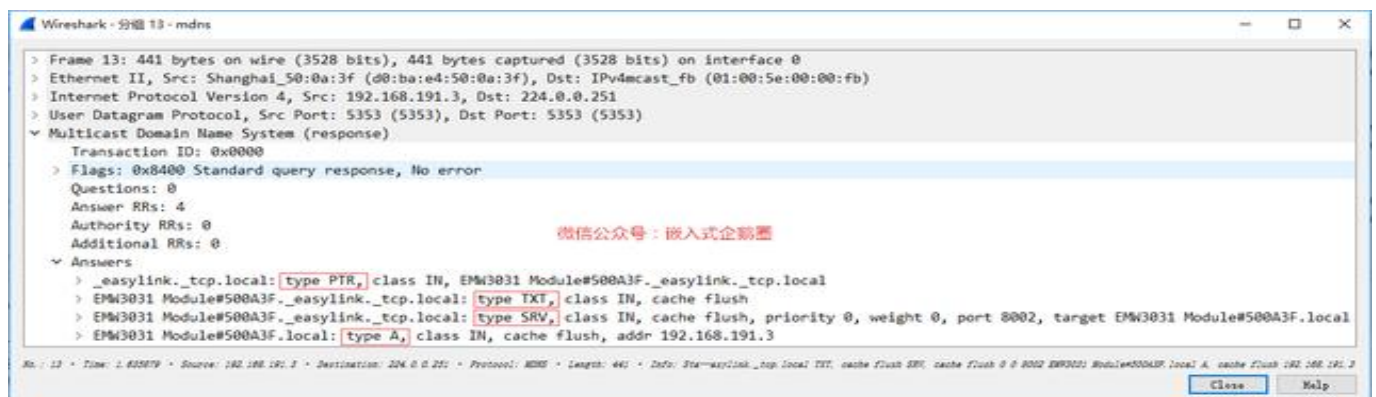
### 三、mDNS數據包

慶科物聯的設備端已經實現了Bonjour協議的主要功能，以下是基於其設備端發現過程用Wireshark抓的包，其中IP位址為192.168.191.2表示的是手機端，192.168.191.3表示的是完成配網後的設備端，它們在同一個區域網內。

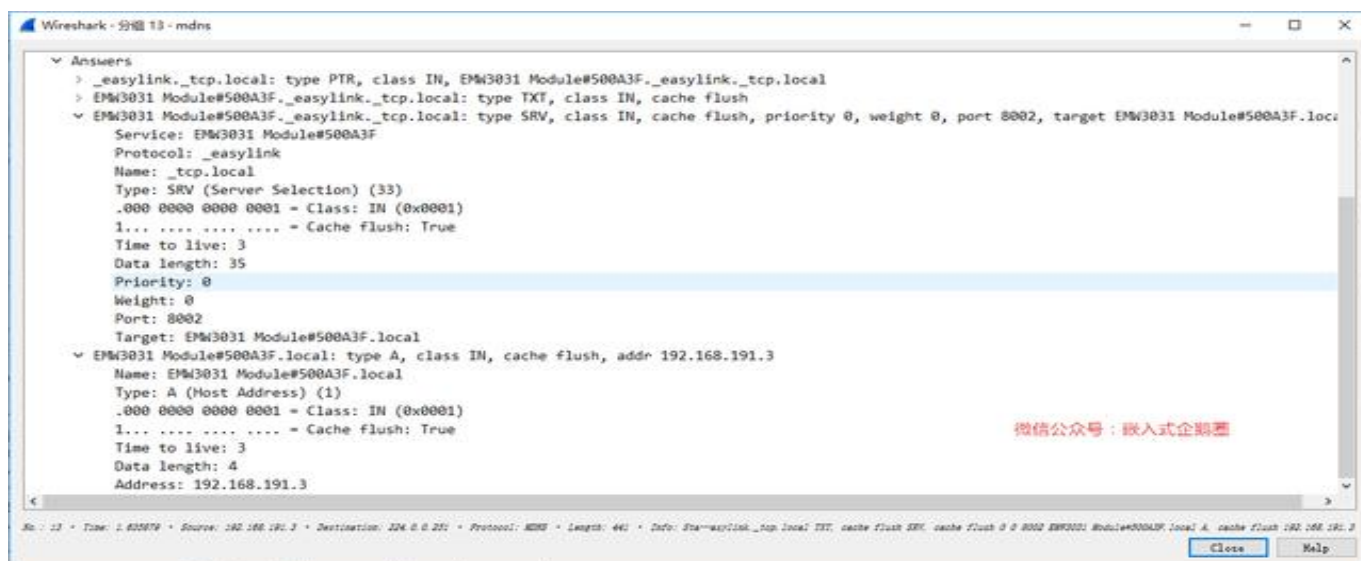
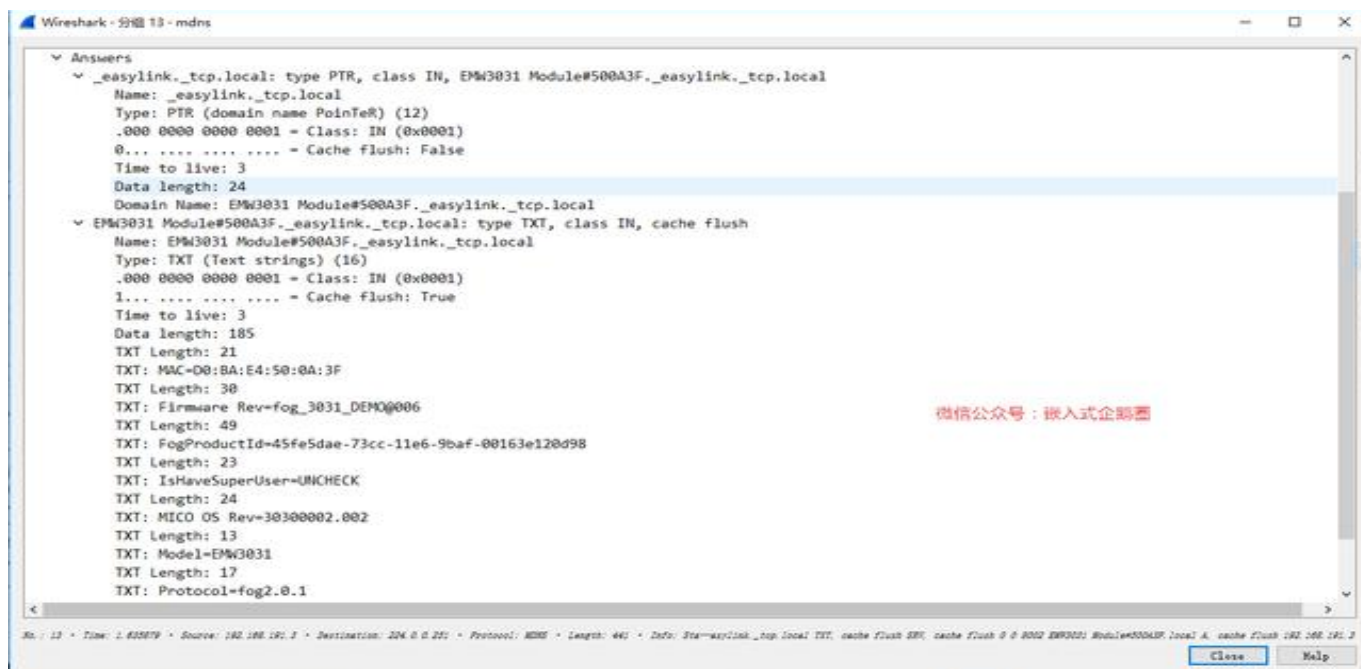
服務發現：由手機APP發送查詢\_easylink.\_tcp.local服務



服務解析：設備端一次性響應了PTR記錄、SRV記錄、TXT記錄以及A記錄：



每條記錄展開為：



歡迎關注微信公眾號：嵌入式企鵝圈，實時推送原創文章！

嵌入式企鵝圈原創團隊由阿里、魅族、nvidia、龍芯、炬力、拓爾思等資深工程師組成。百分百原創，分享嵌入式、Linux、物聯網、GPU、Android、自動駕駛等技術。